UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/558,022	04/25/2000	Takatoshi Ono	NAK1-BK74	9324

21611 7590 07/01/2004

SNELL & WILMER LLP
1920 MAIN STREET
SUITE 1200
IRVINE, CA 92614-7230

EXAMINER	
SHERKAT, AREZOO	

ART UNIT	PAPER NUMBER
2131	6

DATE MAILED: 07/01/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/558,022	ONO ET AL.
	Examiner	Art Unit
	Arezoo Sherkat	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 April 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☒ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-10 are considered for examined.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1-3, and 9-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ashe, (U.S. Patent No. 6,014,745 and Ashe hereinafter) in view of Shimizu et al., (U.S. Patent No. 6,085,323 and Shimizu hereinafter), in further view of Kotani et al., (U.S. Publication No. 2001/0008016 and Kotani hereinafter).

Regarding claims 1, 9, and 10, Ashe discloses a secure system that

(1) reads a type 1 key (i.e., Master Key) from a storage unit (i.e., memory) and (a) main data (i.e., programs and/or data)(Col. 1, lines 35-65);

(b) an encrypted type 2 key (i.e., unique key) produced by encrypting a type 2 key using the type 1 key (i.e., the unique key is encrypted using a master encryption algorithm and can only be obtained

using the master key with the master algorithm)(Col. 2, lines 49-67 and Col. 3, lines 1-15); and

(c) encrypted condition information produced by encrypting condition information using the type 2 key (i.e., unique key) from a recording medium (Col. 1, lines 35-65 and Col. 3, lines 10-15),

(2) decrypts the encrypted condition information using the type 2 key(Col. 3, lines 10-15);

(3) controls usage of the read main data based on the condition information (i.e., proprietary algorithm)(Col. 1, lines 55-65).

Ashe does not expressly disclose updating means and method for updating the type 1 key and a generating means and method for generating a new type 2 key in accordance with usage of the read main data and replacing them on the recording medium with the new ones, although he mentions that as an alternative the algorithm unique to the program being encrypted may be encrypted as well (Col. 3, lines 10-15).

However, Shimizu discloses updating means and method for updating the type 1 key (i.e., plurality of master keys exist each of which may be updated upon authentication of a password)(Col. 13, lines 14-53); and

a generating means and method for generating a new type 2 key in accordance with usage of the read main data (i.e., a master key is used in encrypting a temporary key in the external storage device), and encrypting means and method for encrypting the updated condition information using the new type 2 key and replacing the encrypted condition information on

the recording medium with the encrypted updated condition information, and encrypting means and method for encrypting the new type 2 key using the updated type 1 key and replacing the encrypted type 2 key on the recording medium with the encrypted new type 2 key(Col. 13, lines 54-67 and Col. 14, lines 1-67 and Col. 15, lines 1-13).

Ashe or Shimizu does not disclose updating means and method for updating the condition information.

However, Kotani discloses updating means and method for updating the condition information (Page 5, Par. 0080-0081).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Ashe with the teachings of Shimizu because it would allow to include updating means and method for updating the type 1 key with the motivation to provide for internally defined personal master keys (Shimizu, Col. 13, lines 14-25) and to modify the combined teachings of Ashe and Shimizu with the teachings of Kotani because it would allow to include updating means and method for updating the condition information with the motivation to provide for reissue and update of license information (Kotani, Page1, Par. 0010-0011).

Regarding claims 2 and 3, Ashe discloses a secure system that

(1) reads a type 1 key (i.e., Master Key) from a storage unit (i.e., memory) and (a) main data (i.e., programs and/or data)(Col. 1, lines 35-65) (b) an encrypted type 2 key (i.e., unique key) produced by encrypting

a type 2 key using the type 1 key (i.e., the unique key is encrypted using a master encryption algorithm and can only be obtained using the master key with the master algorithm)(Col. 2, lines 49-67 and Col. 3, lines 1-15), and(c) encrypted condition information produced by encrypting condition information using the type 2 key (i.e., unique key) from a recording medium on which n (where n is an integer no less than two) sets of main data(i.e., proprietary information such as programs and/or data), an encrypted type 2 key, and encrypted condition information are recorded (Col. 1, lines 35-65 and Col. 3, lines 10-15),

(2) decrypts the encrypted condition information using the type 2 key (i.e., unique key)(Col. 3, lines 10-15), and

(3) controls usage of the read main data based on the condition information (i.e., proprietary algorithm)(Col. 1, lines 55-65),

Ashe does not expressly disclose a first and second updating means for updating the condition information and the type 1 key and a generating means for generating a new type 2 key in accordance with usage of the read main data and replacing them on the recording medium with the new ones, although he mentions that as an alternative the algorithm unique to the program being encrypted may be encrypted as well (Ashe, Col. 3, lines 10-15).

However, Shimizu discloses updating means and method for updating the type 1 key (i.e., plurality of master keys exist each of which may be updated upon authentication of a password)(Col. 13, lines 14-53); and

first encrypting means for encrypting the updated condition information using the new type 2 key and replacing the encrypted condition information on the recording medium with the encrypted updated condition information (Col. 7, lines 50-67 and Col. 8, lines 1-24), and second encrypting means for encrypting the new type 2 key using the updated type 1 key and replacing the encrypted type 2 key on the recording medium with the encrypted new type 2 key (Col. 13, lines 54-67 and Col. 14, lines 1-67 and Col. 15, lines 1-13).

Ashe or Shimizu does not disclose updating means and method for updating the condition information.

However, Kotani discloses updating means and method for updating the condition information (Page 5, Par. 0080-0081).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Ashe with the teachings of Shimizu because it would allow to include updating means and method for updating the type 1 key with the motivation to provide for internally defined personal master keys (Shimizu, Col. 13, lines 14-25) and to modify the combined teachings of Ashe and Shimizu with the teachings of Kotani because it would allow to include updating means and method for updating the condition information with the motivation to provide for reissue and update of license information (Kotani, Page1, Par. 0010-0011).

2. Claims 5 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ashe, (U.S. Patent No. 6,014,745 and Ashe hereinafter) and Shimizu et al., (U.S. Patent No. 6,085,323 and Shimizu hereinafter) and Kotani et al., (U.S. Publication No. 2001/0008016 and Kotani hereinafter), in view of Inazawa et al., (U.S. Patent No. 6,587,948 and Inazawa hereinafter).

Teachings of Ashe and Shimizu and Kotani have been disclosed previously.

Regarding claim 5, Ashe or Shimizu or Kotani does not expressly disclose a type 3 encryption key to encrypt the main data.

However, Inazawa discloses wherein the main data in each set on the recording medium has been encrypted using a type 3 encryption key (i.e., a disc key DK)(Col. 5, lines 64-67 and Col. 6, lines 1-11), and obtaining means for obtaining the type 3 encryption key (i.e., the disc key)(Col. 6, lines 57-63); and

second decrypting means for decrypting the read main data using the obtained type 3 encryption key (Col. 6, lines 57-63).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Ashe and Shimizu and Kotani with the teachings of Inazawa because it would allow to include a type 3 encryption key for encrypting main data with the motivation to be capable of effectively preventing illegal copies (Inazawa, Col. 2, lines 56-57).

Regarding claim 6, Ashe or Shimizu or Kotani does not expressly disclose a type 3 encryption key to encrypt the main data.

However, Inazawa discloses wherein the main data in each set on the recording medium has been encrypted using a type 3 encryption key (i.e., a disc key DK) that is unique to the data usage controlling apparatus (Col. 1, lines 65-67 and Col. 2, lines 1-30), and storing means for storing the type 3 encryption key (i.e., the disc key)(Col. 5, lines 64-67 and Col. 6, lines 1-11); and

second decrypting means for decrypting the read main data using the obtained type 3 encryption key (Col. 6, lines 57-63).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Ashe and Shimizu and Kotani with the teachings of Inazawa because it would allow to include a type 3 encryption key for encrypting main data with the motivation to be capable of effectively preventing illegal copies (Inazawa, Col. 2, lines 56-57).

3. Claims 4, 7, and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ashe, (U.S. Patent No. 6,014,745 and Ashe hereinafter) and Shimizu et al., (U.S. Patent No. 6,085,323 and Shimizu hereinafter) and Kotani et al., (U.S. Publication No. 2001/0008016 and Kotani hereinafter), in view of Marino et al., (U.S. Patent No. 6,026,165 and Marino hereinafter).

Teachings of Ashe and Shimizu and Kotani have been disclosed previously.

Regarding claim 4, Ashe discloses when the generating means has not generated a new type 2 key, the first encrypting means re-encrypts the updated condition information using a same type 2 key as was used to decrypt the encrypted condition information (Col. 2, lines 49-67 and Col. 3, lines 1-15).

Ashe or Shimizu or Kotani does not expressly disclose wherein the generating means generates a new type 2 key every time a user makes a predetermined number of uses of the main data on the recording medium.

However Marino discloses wherein the generating means (i.e., the sequence number generator) generates a new type 2 key every time a user makes a predetermined number of uses of the main data on the recording medium (Col. 7, lines 14-46).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Ashe and Shimizu and Kotani with the teachings of Marino because it would allow to include a means and method of updating and replacing the type 2 key in a predetermined fashion with the motivation to enable the encryption key to be easily changed by a user, thus enhancing the security of the system (Marino, Col. 2, lines 43-46).

Regarding claim 7, Ashe or Shimizu or Kotani does not expressly disclose wherein the updating means updates the type 1 key by performing a predetermined calculation on the read type 1 key.

However, Marino discloses wherein the updating means updates the type 1 key (i.e., the sequence number which is used to create a "superkey") by performing a predetermined calculation on the read type 1 key (Col. 7, lines 14-46).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Ashe and Shimizu and Kotani with the teachings of Marino because it would allow to include a means and method of updating and replacing the type 1 key with the motivation to enable the encryption key to be easily changed by a user, thus enhancing the security of the system (Marino, Col. 2, lines 43-46).

Regarding claim 8, Ashe or Shimizu or Kotani does not expressly disclose wherein the updating means updates the type 1 key by adding one to the read type one key.

However, Marino discloses wherein the updating means updates the type 1 key (i.e., the sequence number which is used to create a "superkey") by adding one to the read type one key (Col. 7, lines 40-46).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined teachings of Ashe and Shimizu and Kotani with the teachings of Marino because it would allow to include a means and method of updating and replacing the type 1 key by adding one to the read type 1 key with the motivation to enable the encryption key to be

easily changed by a user, thus enhancing the security of the system (Marino, Col. 2, lines 43-46).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (703) 305-8749. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 305-3718.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

A. Sherkat

Arezoo Sherkat
Patent Examiner
Group 2131
June 28, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100